Notice of Allowability	Application No.	Applicant(s)	
	09/216,519	KERR ET AL.	
	Examiner	Art Unit	
	Paul Callahan	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *9-16-2004*.

2. ☒ The allowed claim(s) is/are *1-19,21-33,35-50 and 52*.

3. ☐ The drawings filed on _____ are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☒ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☒ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☒ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☒ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *02052005* .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Andrew Caldwell
ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

DETAILED ACTION

Response to Amendment

1. Claims 1-53 were pending in this case at the time of the previous Office Action. Claim 20 has been cancelled by the latest amendment. The Applicant has agreed to the cancellation of claims 34, 51, and 53 via Examiner's amendment. Therefore claims 1-19, 21-33, 35-50, and 52 are pending in this Application and have been examined.

Response to Arguments

2. The Applicant's arguments in traverse of the rejections of claims 34, 51, and 53 are now moot in view of the cancellation of those claims.

Drawings

3. The drawings filed on 12/18/1998 are acceptable subject to correction of the informalities indicated on the attached "Notice of Draftsman's Patent Drawing Review," PTO-948. In order to avoid abandonment of this application, correction is required in reply to the Office action. The correction will not be held in abeyance.

EXAMINER'S AMENDMENT

4. An Examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this Examiner's amendment was given in a telephone interview with Mr. Sidney Johnston on February 4, 2005.

The application has been amended as follows:

IN THE CLAIMS:

Please cancel claims 20, 34, 51, and 53 without prejudice.

Claim 1. (Previously Presented) Apparatus for tightly-coupling hardware data encryption functions with software-based protocol decode processing within a pipelined processor of a programmable processing engine in a network switch, the apparatus comprising: an encryption execution unit contained within the pipelined processor; an ALU contained within the pipelined processor; an instruction decode stage (ID stage), in response to reading an opcode, enables the encryption execution unit to read data from a memory shared by the ALU and the encryption execution unit, and for the encryption execution unit to process the data read from the shared memory; and a multiplexer to select as an output a result of processing by the encryption execution unit rather than a result of ALU processing.

Claim 2. (Original) The apparatus of Claim 1 wherein the encryption execution unit is an encryption tightly coupled state machine (TCSM) unit that is selectively invoked within the pipelined processor.

Claim 3. (Previously Presented) The apparatus of Claim 2, further comprising: native encryption opcodes provided within an instruction set of the pipelined processor to enable selective access to the encryption TCSM unit by software.

Claim 4. (Previously Presented) The apparatus of Claim 3, further comprising: a plurality of busses internal to the pipelined processor and wherein a hardware portion of the interface allows the encryption TCSM unit to utilize the internal buses in response to decode processing of the native encryption opcodes.

Claim 5. (Previously Presented) The apparatus of Claim 4, further comprising: the pipelined processor is a microcontroller core (TMC) processor having a multi-stage pipeline architecture that includes an instruction fetch stage, an instruction decode stage, an execution stage and a memory write-back stage.

Claim 6. (Previously Presented) The apparatus of Claim 5, further comprising: the TMC processor further includes an arithmetic logic unit, at least one internal register, an instruction fetch and decode unit and the encryption TCSM unit organized as a data path.

Claim 7. (Previously Presented) The apparatus of Claim 5 wherein the encryption TCSM unit comprises: a data encryption standard (DES) functional component cooperatively coupled to a sub-key generation functional component.

Claim 8. (Previously Presented) The apparatus of Claim 7 wherein the DES functional component comprises: state machine hardware used to execute each round of a DES function.

Claim 9. (Previously Presented) The apparatus of Claim 7, further comprising: the sub-key generation functional component comprises state machine hardware that generates a sub-key as needed for each round of a DES function.

Claim 10. (Previously Presented) A method for tightly-coupling hardware data encryption functions with software-based protocol decode processing within a pipelined processor of a programmable processing engine in a network switch, the method comprising the steps of: providing an encryption execution unit within the pipelined processor; providing an ALU within the pipelined processor; enabling, by an instruction decode stage (ID stage) in response to reading an opcode, the encryption execution unit to read data from a memory shared by the ALU and the pipelined processor, and for the encryption execution unit to process the data read from the memory; and selecting as output the result of processing by the encryption execution unit rather than selecting results from the ALU.

Claim 11. (Previously Presented) The method of Claim 10, further comprising: having native encryption opcodes contained within an instruction set of the pipelined processor; and issuing the native encryption opcodes directly to the encryption execution unit to substantially reduce encryption setup latency.

Claim 12. (Previously Presented) The method of Claim 11, further comprising: decoding the native encryption opcodes at the instruction decode stage; and in response to the step of decoding, invoking the encryption execution unit to perform encryption/decryption functions at the execution stage.

Claim 13. (Previously Presented) The method of Claim 12, further comprising: protocol processing of protocols contained in a plaintext stored at the network switch to determine an appropriate encryption algorithm; upon determining the appropriate encryption algorithm, immediately starting an operation to fetch initial keys needed to perform the encryption/decryption functions; and upon fetching the keys, providing the keys to the encryption execution unit within the TMC processor.

Claim 14. (Previously-Presented) The method of Claim 13, further comprising: including a plurality of high-performance busses internal to the TMC processor; and accessing the internal busses to simultaneously load an encryption key and store a previous encryption result.

Claim 15. (Previously Presented) The method of Claim 12 further comprising the step of, wherein the encryption execution unit is an encryption tightly coupled state machine

(TCSM) unit: initializing the encryption TCSM unit in response to execution of a first instruction that defines the form of operation to be performed.

Claim 16. (Original) The method of Claim 15 wherein the encryption TCSM unit comprises a data encryption standard (DES) functional component cooperatively coupled to a sub-key generation functional component and wherein the step of initializing comprises the steps of: decoding a first portion of the first instruction to initialize the DES functional component; and decoding a second portion of the first instruction to initialize the sub-key generation functional component.

Claim 17. (Original) The method of Claim 16 further comprising the step of: executing the second instruction having a micro-opcode field containing a native encryption opcode that specifies loading an initial key from a memory into the sub-key generation functional component of the encryption TCSM unit.

Claim 18. (Previously Presented) The method of Claim 17 further comprising the step of: performing a DES function on a plaintext in response to execution of a third instruction having a micro-opcode field containing a native encryption code that specifies loading of the plaintext into the DES functional component of the encryption TCSM unit and initiating DES operations; and upon completing the DES operations, storing a ciphertext result in an internal register coupled to the DES functional component.

Claim 19. (Original) The method of Claim 18 further comprising the step of: executing a fourth instruction to store the ciphertext results contained in the internal register to a location in the memory.

Claim 20. (Canceled)

Claim 21. (Previously Presented) A pipelined processor in a network switch, the processor comprising: an ALU internal to the processor responsive to a first set of opcodes; an encryption execution unit internal to the processor having an encryption tightly coupled state machine (TCSM) responsive to a second set of opcodes; an instruction decode stage (ID stage) to decode an opcode, the ID stage, in response to an opcode of said second set of opcodes, transferring processing to the encryption execution unit; a multiplexer to select output from the ALU OR from the encryption execution unit.

Claim 22. (Previously Presented) The processor of Claim 21, wherein the processor is a microcontroller core (TMC) processor and further comprises: an instruction fetch stage; an execution stage to execute an instruction decoded by the ID stage; and a memory write-back stage to write a result of said execution stage to memory.

Claim 23. (Previously Presented) The processor of Claim 21, further comprises: one or more internal registers; a bus operatively connecting the one or more internal registers to both the ALU and the encryption execution unit; and a multiplexer having inputs from both the ALU and the encryption execution unit, the multiplexer outputting a selected input.

Claim 24. (Previously Presented) The processor of Claim 21, wherein the encryption TCSM unit comprises: a data encryption standard (DES) functional component cooperatively coupled to a sub-key generation functional component.

Claim 25. (Previously Presented) The processor of Claim 24, wherein the DES functional component comprises: a state machine that executes each round of a DES function.

Claim 26. (Previously Presented) The processor of Claim 24, wherein the sub-key generation functional component comprises: a state machine that generates a sub-key as needed for each round of a DES function.

Claim 27. (Previously Presented) A method for providing encryption functions within a pipelined processor in a network switch, the method comprising the steps of:

associating a first set of opcodes with an ALU internal to the processor, the ALU performing protocol processing operations;

associating a second set of opcodes with an encryption execution unit internal to the processor, the encryption execution unit performing encryption operations;

decoding opcodes by an instruction decode stage (ID stage); transferring by the ID stage, in response to an opcode from said first set of opcodes, processing to the ALU; transferring by the ID stage, in response to an opcode from said second set of opcodes, processing to the encryption execution unit; and selecting output from the ALU OR from the encryption execution unit.

Claim 28. (Previously Presented) The method of Claim 27, further comprises the step of: providing one or more internal registers; providing a bus operatively connecting the one or more internal registers to both the ALU and the encryption execution unit; providing a multiplexer having inputs from both the ALU and the encryption execution unit, the multiplexer outputting a selected input.

Claim 29. (Previously Presented) The method of Claim 27 further comprising the step of: initializing the encryption TCSM unit in response to a first instruction that defines a form of operation to be performed.

Claim 30. (Previously Presented) The method of Claim 29, wherein the step of initializing comprises the steps of: decoding a first portion of the first instruction to initialize a DES functional component; and decoding a second portion-of the first instruction to initialize a sub-key generation functional component.

Claim 31. (Previously Presented) The method of Claim 27, further comprising the steps of: executing a second instruction including an encryption opcode that specifies loading an initial key from a memory into a sub-key generation functional component of the TCSM unit.

Claim 32. (Previously Presented) The method of Claim 27, further comprising the steps of: performing a DES function in response to execution of a third instruction having a field containing an encryption opcode that specifies loading plaintext and initializing a DES operation.

Claim 33. (Previously Presented) A computer readable media, comprising:
said computer readable media containing instructions for execution in a processor for the practice of the method of,

providing a tightly-coupling hardware data encryption function with software based protocol decode processing within a pipelined processor of a programmable processing engine in a network switch; providing an encryption execution unit within the pipelined processor; providing an ALU within the pipelined processor; enabling, by an instruction decode stage (ID stage) in response to reading an opcode, the encryption execution unit to read data from a memory shared by the ALU and the pipelined processor, and for the encryption execution unit to process the data read from the memory; and

selecting as output the result of processing by the encryption execution unit rather than selecting results from the ALU.

Claim 34. (Canceled)

Claim 35. (Previously Presented) A router, comprising: a processor having an Instruction decode stage (ID stage) for processing opcodes; an ALU for performing protocol processing operations; a tightly coupled state machine (TCSM) for performing encryption processing; a shared memory for providing data to either the ALU or the TCSM; the ID stage, in response to reading an opcode, transferring processing to the TCSM, and the TCSM performing encryption processing on data read from the shared memory; a selector to select as output results from the ALU OR results from the TCSM.

Claim 36. (Previously Presented) The apparatus of Claim 35, further comprising: the selector is a multiplexer.

Claim 37. (Previously Presented) The apparatus of Claim 35, further comprising; the

ALU selects whether the ALU or the TCSM reads data from the memory.

Claim 38. (Previously Presented) The apparatus of Claim 35, further comprising: the TCSM performs DES data encryption standard encryption processing.

Claim 39. (Previously Presented) The apparatus of Claim 35, further comprising: a sub-key generation component to provide a key to the TCSM.

Claim 40. (Previously Presented) A method for operating a router, comprising: processing opcodes by an instruction decode stage (ID stage); performing encryption processing by a tightly coupled state machine (TCSM); performing protocol processing by an ALU; reading data from a shared memory by either the ALU or the TCSM; transferring processing by the ID stage, in response to reading an opcode to the TCSM, and the TCSM performing encryption processing on data read from the shared memory; selecting as output results from the ALU OR results from the TCSM.

Claim 41. (Previously Presented) The method of Claim 40, further comprising: using a multiplexer for selecting as output results from the ALU OR results from the TCSM.

Claim 42. (Previously Presented) The method of Claim 40, further comprising; selecting whether the ALU or the TCSM reads data from the memory.

Claim 43. (Previously Presented) The method of Claim 40, further comprising: performing DES data encryption standard encryption processing by the TCSM.

Claim 44. (Previously Presented) The method of Claim 40, further comprising: providing a key to the TCSM by a sub-key generation component.

Claim 45. (Previously Presented) A router, comprising: means for providing a processor having an ALU for processing opcodes and a tightly coupled state machine (TCSM) for performing encryption processing; means for reading data from a shared memory by either the ALU or the TCSM; means for transferring processing by an instruction decode stage (ID stage), in response to reading an opcode, to the TCSM, and the TCSM performing encryption processing on data read from the shared memory; means for selecting as output results from the ALU OR results from the TCSM.

Claim 46. (Previously Presented) The apparatus of Claim 45, further comprising: means for using a multiplexer for selecting as output results from the ALU OR results from the TCSM.

Claim 47. (Previously Presented) The apparatus of Claim 45, further comprising; means for selecting by the ALU whether the ALU or the TCSM reads data from the memory.

Claim 48. (Previously Presented) The apparatus of Claim 45, further comprising: means

for performing DES data encryption standard encryption processing by the TCSM.

Claim 49. (Previously Presented) The apparatus of Claim 45, further comprising: means for providing a key to the TCSM by a sub-key generation component.

Claim 50. (Previously Presented) A computer readable media, comprising:

said computer readable media containing instructions for execution in a processor for the practice of the method of,

providing encryption functions within a pipelined processor in a network switch, having the steps,

associating a first set of opcodes with an ALU internal to the processor, the ALU performing protocol processing operations;

associating a second set of opcodes with an encryption execution unit internal to the processor, the encryption execution unit performing encryption operations;

decoding opcodes by an instruction decode stage (ID stage);

transferring by the ID stage, in response to an opcode from the first set of opcodes, processing to the ALU;

transferring by the ID stage, in response to an opcode from said second set of opcodes, processing to the encryption execution unit; and selecting output from the ALU OR from the encryption execution unit.

Claim 51. (Canceled)

Claim 52. (Previously Presented) A computer readable media, comprising: said Computer readable media containing instructions for execution in a processor for the practice of the method of operating a router, having the steps, processing opcodes by an instruction decode stage (ID stage); performing encryption processing by a tightly coupled state machine (TCSM); performing protocol processing by an ALU; reading data from a shared memory by either the ALU or the TCSM; transferring processing by the ID stage, in response to reading an opcode to the TCSM, and the TCSM performing encryption processing on data read from the shared memory; and electing as output results from the ALU OR results from the TCSM.

Claim 53. (Canceled)

In The Specification:

Replace lines 12-15 appearing on page 10 of the Specification with the following:

present invention is described in ~~copending and~~ commonly-owned US Patent ~~Application Serial~~ No. ~~(112025-77)~~ 6,513,108, issued January 28, 2003, titled *Programmable Arrayed Processing Engine Architecture for a Network Switch*, which ~~application~~ is hereby incorporated by reference as though fully set forth herein.

Allowable Subject Matter

5. Claims 1-19, 21-33, 35-50, and 52 are allowed.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The following US Patent Documents teach systems of data processing similar to the applicant's invention.

Bernet et al. 5,764,645

Sasaki et al. 5,113,503

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Andrew Caldwell, can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is: (703) 872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Andrew Caldwell

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER

2/5/05

Paul Callahan